

THE CLAIMS:

1 (previously presented). A method for providing authentication or identification services to a first user regarding a second user, the method comprising:

- establishing a telephone call between the first user and the second user through a media gateway;
- detecting a voice command from the first caller during the telephone call;
- requesting a certificate corresponding to the second user from an authentication server in response to the voice command;
- returning the certificate corresponding to the second user;
- requesting authentication of the certificate corresponding to the second user from a control program associated with the second user;
- returning an authentication certificate from the control program associated with the second user; and
- verifying authentication by comparing the authentication certificate corresponding to the second user and received from the control program associated with the second user with the certificate received from the authentication server.

2. (original). The method according to claim 1, wherein the first user communicates with the second user through a media gateway.

3 (original). The method according to claim 1, further comprising monitoring the communication between the first user and the second user so that the authentication server may notify the first user if the second user changes or becomes untrustworthy.

4 (original). The method according to claim 1, wherein the requesting of the certificate corresponding to the second user from the authentication server, requesting authentication of the certificate corresponding to the second user and the verifying authentication is performed by a control program associated with the first user.

5 (original). The method according to claim 1, wherein the first and second users are using client devices configured to communicate with each other and with the authentication server.

6 (original). The method according to claim 5, wherein the client devices are smart phones.

7 (original). The method according to claim 1, wherein the authentication server has authenticated an organization and the second user is a member of the authenticated organization.

8 (original). The method according to claim 1, wherein verifying authentication determines a level of trust between the first user, the authentication server and the second user.

9 (original). The method according to claim 8, wherein the level of trust is a value corresponding to the probability that the authentication certificate corresponding to the second user and received from the control program associated with the second user is the same as the certificate received from the authentication server.

10 (original). The method according to claim 1, wherein the authentication certificate corresponding to the second user and received from the control program associated with the second user includes a portion indicating the second user's identity.

11 (previously presented). A system for facilitating authentication services comprising:

an authentication server configured to provide an authentication certificate to a user of a first client device for authentication or identification of a user of a second client device, the first and second client devices being configured to communicate with each other and the authentication server, each of the first and second client devices including a user control program configured to communicate data to and from the authentication server, and a media gateway coupled to the authentication server and enabling communication of media data from the first and second client devices to the authentication server,

wherein, the user control program of the first client device, in response to a voice command of the first user requesting authentication of the second user, is configured to receive a certificate corresponding to the user of the second client device and the authentication certificate from the authentication server and being configured to authenticate the user of the second client device by comparing the certificate corresponding to the second client device and the authentication certificate.

12 (original). The system according to claim 11, wherein the authentication server is configured to monitor the communication between the first user and the second user.

13 (original). The system according to claim 11, wherein the authentication server is configured to continuously monitor the communication between the first user and the second user so as to notify the first user if the second user changes or becomes untrustworthy.

14 (original). The method according to claim 11, wherein the control program associated with the first user is configured to request the certificate corresponding to the second user from the authentication server, request authentication of the certificate corresponding to the second user and verify authentication.

15 (previously presented). The system according to claim 11, wherein the first and second users use client devices configured to communicate with each other and with the authentication server.

16 (original). The system according to claim 15, wherein the client devices are smart phones.

17 (original). The system according to claim 11, wherein the authentication server has authenticated an organization and the second user is a member of the authenticated organization.

18 (original). The system according to claim 14, wherein verifying authentication determines a level of trust between the first user, the authentication server and the second user.

19 (original). The system according to claim 18, wherein the level of trust is a value corresponding to the probability that the authentication certificate corresponding to the second user and received from the control program associated with the second user is the same as the certificate received from the authentication server.

20 (original). The system according to claim 11, wherein the authentication certificate corresponding to the second user and received from the control program associated with the second user includes a portion indicating the second user's identity.

21-47 (cancelled).